## IN THE SPECIFICATION

**Amendments to the Specification:**

Please amend the paragraphs starting at the following identified locations, in the as-filed application.

Page 20, line 3:

Directing attention to FIGS. 3 and 4, the security contract 200 between the application server 202 and resource adapter 204 extends the connection management contract by adding security specific details. This security contract 200 supports EIS sign-on by passing the connection request from the resource adapter 204 to the application server 202 and enabling latter to hook-in security services. The security contract 200 also provides for propagation of security context (JAAS Subject, its principals and credentials) from the application server 202 to the resource adapter 204. The security contract 200 includes the following classes and interfaces: subject 206 ~~106~~, generic credential, password credential, connection manager, managed connection factory, and managed connection.

Page 20, line 11:

Subject 206 ~~106~~ represents a grouping of related information for a single entity, such as a person. Such information includes the subject 206's ~~106's~~ identities as well as its security related attributes (for example, passwords and cryptographic keys). Subject 206 ~~106~~ can have multiple identities. Each identity is represented as a principal within the subject 206 ~~106~~. A principal simply binds a name to subject 206 ~~106~~. Subject 206 ~~106~~ may also own security related attributes, which are referred to as credentials. Sensitive credentials that require special protection, such as private cryptographic keys, are stored within a private credential set. The credentials intended to be shared, such as public key certificates or Kerberos server tickets, are stored within a public credential set. Different permissions are required to access and modify different credential sets. The getPrincipals method is used to retrieve all the principals associated with subject 206 ~~106~~. The methods getPublicCredentials and getPrivateCredentials are used respectively to retrieve all the public or private credentials belonging to Subject 106. The methods defined in the set class are used to modify the returned set of principals and credentials.

Page 21, line 1:

The interface java. security. Principal 210 ~~110~~ is used to represent a resource principal. The following code extract is an illustrative example showing the principal interface:

Page 21, line 9:

The method getName returns the distinguished name of a resource principal. An application server 202 should use an implementation of the principal interface to pass a resource principal as part of subject 206 ~~106~~ to a resource adapter 204. The interface javax. resource. spi.

security. GenericCredential defines a security mechanism independent interface for accessing security credential of a resource principal.

Page 21, line 14:

The GenericCredential interface 208 ~~108~~ provides as a Java wrapper over an underlying mechanism specific representation of a security credential. The GenericCredential interface 208 ~~108~~ enables a resource adapter 204 to extract information about a security credential. The resource adapter 204 can then manage EIS sign on for a resource principal. The following code extract example shows the GenericCredential interface 208:

Page 23, line 3:

The java. security. Principal interface 210 ~~110~~ represents a resource principal. The PasswordCredential class is required to implement equals and hashCode method. The following code segment is an illustrative example.

Page 25, line 20:

The application server 202 has several options for invocation of the method createManagedConnection: Option A: The application server 202 invokes the method createManagedConnection by passing in a non null Subject instance that carries the resource principal and its corresponding password based credential (represented by the class PasswordCredential, which provides the user name and password). The resource adapter 204 extracts the user name and password from this Subject instance (by looking for PasswordCredential instance in the Subject 206 ~~106~~) and uses this security information to sign-on to the EIS instance during the connection creation. Option B: The application server 202 invokes the method createManagedConnection method by passing in a nonnull Subject instance that carries the resource principal and its credentials. In this option, credentials are represented through the GenericCredential interface 208. A typical example is a Subject instance with Kerberos credential. For example, an application server can use this option for createManagedConnection method invocation when the resource principal is impersonating the caller/initiating principal and has valid credentials acquired through impersonation. An application server can also use this option for principal mapping scenarios with credentials of a resource principal represented through the GenericCredential interface 208. The resource adapter 204 uses the resource principal and its credentials from the Subject instance to go through the EIS sign-on process before creating a new connection to the EIS. Option C: The application server 202 requests resource adapter 204 to manage the EIS sign-on by passing a null Subject instance. The application server 202 uses this option for the component managed sign on case where security information is carried in the ConnectionRequestInfo instance. The application server 202 does not provide any security information that can be used by the resource adapter 204 for managing EIS sign-on.

Page 27, line 14:

Option B: The resource adapter 204 explicitly checks whether passed Subject instance carries a GenericCredential instance using the methods getPrivateCredentials and getPrivateCredentials defined on the Subject 206 ~~106~~ interface. Note that sensitive credentials that require special protection, such as private cryptographic keys, are stored within a private credential Set. While credentials intended to be shared, such as public key certificates or Kerberos server tickets, are stored within a public credential Set. The two methods

getPrivateCredentials and getPrivateCredentials should be used accordingly. The resource adapter 204 uses the resource principal and its credentials (as represented through the GenericCredential interface) in the Subject instance to go through the EIS sign-on process. For example, this option is used for Kerberos based credentials that have been acquired by the resource principal through impersonation.